

## SYSTEMS FOR STORING AND TRANSFERRING DATA

The present invention refers to systems of storing and transferring data confidentially and personally by means of portable independent electronic objects; it refers more particularly to these portable electronic objects.

In the U.S. application Ser. No. 560,873, U.S. Pat. No. 3,971,916, filed on the Mar. 21, 1975 by the Applicants a system was described which is composed:

on the one hand of at least one portable independent electronic object,

on the other hand of at least one transfer device.

The portable object comprises:

at least one store intended for the storage of data in an easily portable form containing enabling data, coupling means accessible from outside the portable object, enabling the said portable object to be coupled temporarily with the said transfer device, circuits for control of the store, interconnected between the coupling means and the store.

The store and the control circuits of the portable object are produced in the form of logical microstructures.

The transfer device includes means of transfer of data into or out of the portable object; it includes in addition an identification comparator which compares the enabling data contained in the store with a confidential item of data introduced into the transfer device by the bearer of the portable object.

These systems may be employed especially in banks or sales points for distributing banknotes or for allowing a transaction between, for example, a tradesman and a buyer. In the latter case the buyer has available a portable object in the form of a payment card. In order to settle the amount of his purchases he couples his payment card to the transfer device which is, for example, associated with the tradesman's cash-register.

In the electronic stores on the card are recorded a confidential enabling code enabling the identity of the owner of the payment card to be identified, the identity of the client (his bank account number, the name of the client), the succession of debit and credit operations carried out by the transfer device.

The confidential enabling code is, for example, recorded in the payment card in the form of a word of several bits. The user of the payment card who is the only one to know the confidential number corresponding with the enabling data contained in the card introduces (for example, by means of a keyboard) this confidential number into the transfer device. The identification comparator contained in this transfer device compares this confidential code number with the enabling data contained in the payment card, thus authenticating the identity of the user of the card prior to the debit and credit operations. In the case where the confidential code number introduced by the bearer of the card into the transfer device does not correspond with the word of several bits recorded in the payment card the identification comparator interrupts the continuation of the operations (debit, credit, etc.) being carried out by the transfer device. One is thus assured that the transaction really concerns the regular holder of the payment card.

However, elaborate though this system is, it exhibits one disadvantage which it is desirable to eliminate. That

is, a swindler who is a specialist in microelectronics has the possibility of achieving a simplified version of the transfer device, designed to apply voltage to the portable object and depending on the wish of the Swindler, to read or write information in the store of the portable object. Thus, for example, in the case of a stolen payment card the swindler does not need to know the confidential enabling code to read the contents of the store of the portable object or to modify it.

In the co-pending Application filed on the same day at the same time with the title: "System of transferring and storing data personally and confidentially by means of portable independent electronic objects", a portable object was described which to a large extent eliminates the disadvantages which have just been explained. This portable object includes an identification comparator connected with the store and the coupling means, which is intended to compare the enabling data contained in the store with a confidential item of data introduced into the transfer device by the bearer of the portable object.

Thanks to this identification comparator located inside the portable object the swindler no longer has the possibility of reading or modifying the contents of the portable object which he has found or stolen. That is, he must prior to any operation provide the confidential code and introduce it into the portable object by means of the transfer device, which for him is impossible since only the regular holder of the portable object knows the confidential code.

This portable object is particularly well adapted to combat attempts at fraud when the enabling data consist of a word of great length composed of several digits. That is, even if the swindler puts to work a programmed automatic equipment to apply to the portable object a combinative series of every possible confidential code he will need a considerable time for discovering the enabling data contained in the card. For example, in the case of a confidential code of 50 bits he will need 230 years if he has available an automatic equipment having a clock frequency of 1 MHz.

However, a long confidential code compels users in normal operation to compose on a numerical keyboard a large number of digits (13 in the quoted example) or else on an alphabetical keyboard an equally long succession of letters (10 in the quoted example).

If in order to facilitate the employment of the portable object the number of digits in the confidential code is reduced one then makes again possible, fraud by means of a programmed automatic equipment. For example, in the case of a confidential code of four digits (16 bits in BCD code) it will be sufficient for the swindler to generate in the worst case a series of 10,000 confidential codes of 16 bits, or 160,000 bits; if he has available an automatic equipment operating at the frequency of 1 MHz a time of operation of 0.16 s is sufficient. Similarly, in the case of a confidential code of seven letters the time necessary to the automatic equipment will be of the order of 78 hours, which is still suitable to a swindler.

The aim of the present invention is to correct this disadvantage and to avoid a particularly well equipped and informed swindler being able with impunity to subject a found or stolen portable object to a series of ultra-rapid systematic tests with every possible confidential code until the access gates to the store of the portable object open.